The rise of deep fakes and how to protect your business

---

1. Research found that 41% of images analysed contained disinformation.

2. Fraudsters use a portion of truth to create misleading deep fakes, so it appeals to people's confirmation bias.

3. There are 3 ways to protect your business, including keeping up to date on fraudsters' tricks and monitoring your brand online.

'You have to see it to believe it' no longer applies. The rise and rise of the technology to create deep fakes means businesses need to be vigilant and take precautions to prevent costly confidence tricks. **Steve Pikett** and **Rylee Muddle** explain how you can protect your business.

Imagine this:

You receive a video message from your CFO: "On holiday in the Maldives, we need to pay our web registration bill today or we lose our domain name. It's not a lot, just under $7,500, so arrange to send the money pronto to……"

No reason to doubt its veracity, after all it is no different to many of the emails, voice notes and video messages we all get daily. But it's not real.

"It was her. I know it was, I could see her and hear her talking…" but it's not her. If you take this example to the nasty extreme of the personal it could extend to

messages about personal finances, scam insurance claims, even undermining personal relationships and the trust in partners and family. Which could cost a lot more – in money and reputation – than a few thousand.

Whatever the scenario it is designed to be believable yet shocking enough to interrupt your ability to think rationally and introduce some panic. This vastly increases the criminal's chances of making a fast buck – off you or your business.

We all know to pose for photographs with our good side and photoshopped influencers proliferate on social media. However, leaps in technological possibilities and machine learning have raised the stakes well beyond airbrushing. Bad actors are increasingly able to use rapidly evolving technologies more easily to manipulate information to be false or misleading. One such technology is **deep fake** video and voice, which is being coupled with artificial intelligence (AI) to create very convincing videos to promote a point of view, for financial gain, to sway an election, or to cause harm.

We've seen convincing examples where sampled voices matching a person's normal style have been used to create a 'deep fake'. One example had the parents of a student who was 'deep faked' claiming it really was their daughter speaking in the footage. Even after they were told it was a deep fake, the parents had to check in with their daughter and verify it was not her.

Released early in March, a piece of research by **The Center for Countering Digital Hate** created 40 text prompts on the theme of the upcoming U.S. election in November and ran 160 tests across four popular AI image tools. In 41% of cases, the image returned contained election disinformation, including fake images about candidates and election fraud. These results show just how easy it is for anyone – with malicious intent or not – to create content that isn't based in fact.

These fakes – which reach across all areas of our lives – are often cleverly edited with genuine video footage to increase the possibility of the fake being taken as fact. The very tools used to promote goods and services are being used by bad actors to add credibility to a fake message. Along with marketing techniques, advertising and psychology, another trick is to use inferred knowledge. This is done by adding behavioural science to known data points with AI, this creates messages which the recipients are more likely to accept. Often this way of

spreading false or misleading information feeds confirmation bias, making it even more likely the person will believe it and might even ignore the fakery if they spot it.

Confirmation bias, which is the likelihood you will believe something as it already aligns with your preconceptions or preferences, can be used to particularly damaging effect during elections for example – so in a year like this one when two billion people in more than 80 countries are going – or have been – to the polls, it could literally be a regime changer. The way to manage it is to be aware of your own biases and seek out different perspectives using reliable sources of information, then evaluate the evidence critically. The way algorithms work doesn't support this approach as they are designed to feed you more of what you like or agree with.

Fraudsters not only gain credibility by inserting genuine content, but often by duping real and trusted promoters to set the tone, often without their full knowledge or backing. They also target groups of conspiracy theorists to support and spread a message. All these techniques are used to propagate conspiracy theories, discredit political opponents, and to change a narrative from an understood and accepted position to where it is brought into question.

The best way for businesses to protect themselves is through education and robust systems. It is important to make your people aware of the tactics used by fraudsters and to educate employees on how to spot deep fakes. It is also important to have strong security measures in place, such as multi-factor authentication and verification processes for financial transactions. Additionally, businesses can monitor their online presence to quickly identify and address any deep fakes that may be circulating.

How deep fakes are created:

Deep fakes are created using advanced machine learning techniques, specifically a type of neural network called a generative adversarial network (GAN). GANs consist of two neural networks, a generator and a discriminator, that work together to create realistic synthetic media. The generator creates new data samples, while the discriminator evaluates them for authenticity. The two networks are trained together in a process where the generator tries to create increasingly realistic data, while the discriminator becomes better at detecting fakes. This process continues until the generator produces data that is

indistinguishable from real data. In the case of deep fakes, the generator creates synthetic videos or audio, while the discriminator evaluates their realism.

3 ways to protect your business:

- **Be aware of the tactics used by fraudsters:** Businesses should educate their employees on how to spot deep fakes and the techniques used to enhance their credibility, such as marketing, advertising, psychology, and inferred knowledge.
- **Have strong security measures in place:** Businesses should implement multi-factor authentication and verification processes for financial transactions, with sensitive communications while reducing reliance on video or voice messages. Though it may seem dated, talking directly to a person you know, in video or on a call, can be an effective protection. Deep fakes tend to behave strangely in real-time conversation and it "just doesn't feel like the real person". Trust your instincts.
- **Monitor online presence and reputation:** Businesses should track and address any deep fakes that may be circulating online that could harm their brand, image, or credibility, and report them to the relevant authorities or platforms.

Deep fakes are a growing concern in all spheres of our lives. For businesses, being aware of the tactics used by fraudsters and taking out proactive measures as well as keeping up to date with technological advances, can help mitigate these risks. One adage that does still apply is, if it seems too good to be true, it probably is.

To discuss any of the points raised in this article or to find out how Aztec's risk and innovation team is working to protect our clients, please contact **Steve** and **Rylee**.